Remarks/Arguments

In the specification, Applicant has amended the Abstract to address several editorial issues. Applicant has not added any new matter.

As detailed above, Applicant has amended claims 2, 3, 31, 34, 35, 53, 54, 58, 69, 73, 79, and 97 to correct minor mistakes.

There are 120 claims pending in this application, including independent claims 1, 28, 29, 30, 40, 68, 70, 80, 96, 100, 105, and 111. The action dated September 1, 2004, rejected each of the original 120 claims pursuant to either 35 U.S.C. § 102 as being anticipated by U.S. Patent No. 6,148,342 (hereinafter Ho) or 35 U.S.C. § 103 as being unpatentable over Ho in view of U.S. Patent No. 4,757,534 (hereinafter Matyas), U.S. Patent No. 5,764,772 (hereinafter Kaufman), and/or U.S. Patent No. 6,199,113 (hereinafter Alegre). Applicant respectfully traverses each and every rejection.

Claims 1-27

The action rejected independent claim 1 pursuant to 35 U.S.C. § 102 as being anticipated by Ho. In order to anticipate claim 1, Ho must set forth either expressly or inherently each and every element of claim 1. Ho fails in this regard and, therefore, Applicant respectfully traverses this rejection.

Claim 1 is directed to a computer readable medium containing a database structure for storage of encrypted data. The claim includes two limitations for the database structure. First, the database structure comprises at least one data entity encrypted by at least one encryption key, the data entity having at least one searchable attribute. Second, the database structure comprises at least one encryption key identification in association with the data entity and corresponding to the

encryption key. Thus, at a minimum, the database structure comprises both an encrypted data entity and information (i.e. an encryption key identification) associated with the data entity that may be used to identify the encryption key used to encrypt the data entity.

Ho describes a system and method for retrieving sensitive stored data. Stated generally, Ho describes a source terminal receiving a request for data about a subject from a user. The source terminal combines information about the subject, the user, and possibly the source terminal itself into an "identifier" that it encrypts using a first encryption key. Next, the source terminal converts the user's request into a "data access request" that it encrypts using a second encryption key. The source terminal then combines the identifier and the data access request to form a data packet and sends the packet to an identifier database. The identifier database has the codes necessary to decrypt the identifier portion of the packet. (Col. 3, lines 51-52.) Using those codes, the identifier database decrypts the identifier and analyzes whether the user is permitted access to the subject's data. The analysis typically includes using the identifier information to lookup records in a table. Thereafter, if the user is permitted access, the identifier database prepares a second data packet containing a subject data section and the data access request, with the subject data section including a user access level and an internal identifier. The subject data section may also be encrypted. (Col. 4, lines 30-33.) The identifier database then sends the data packet to a data request database that has the codes necessary to decrypt the packet. (Col. 4, lines 43-45.) After decrypting the data packet, the data request database acts on the data request and, if the user has an appropriate access level, transmits the requested information to the source terminal.

Although the system described in Ho does include several databases, Ho does not at any time disclose, teach, or suggest that any of the information contained in the databases is encrypted and, therefore, Ho does not disclose, teach, or suggest a database structure having a data entity encrypted

by at least one encryption key. Ho states that the databases used in its system typically are tables that contain, for example, individually identifiable attributes, user access levels, and internal identifications, and describes using the contents of data packets to look up information in the tables. Ho does not include any additional information about the database contents and certainly does not discuss encrypting the database contents prior to storing that information. In fact, Ho teaches away from encrypting the information stored in the databases when it states that results from database queries may be encrypted before being transmitted to other sections of the system. If the information stored in the databases is already encrypted then there would be no need to encrypt that information again before it is transmitted.

Ho also does not disclose a database structure having at least one encryption key identification in association with a data entity and corresponding to the encryption key used to encrypt the data entity. As already mentioned, Ho does not disclose, teach, or suggest a database having entries that are encrypted, and, therefore, it should be no surprise that Ho also does not disclose storing a corresponding encryption key identification associated with a particular entry. If the information within the databases is not encrypted then there is no encryption key identification to associate with a particular database entry.

Ho does describe preparing and transmitting data packets and states that the information in the data packets is encrypted. However, Ho does not disclose, teach, or suggest that the data packets include, or otherwise have associated with them, information regarding the identification of any encryption key. There is a simple reason for this: in the system described in Ho the components receiving packets already know the codes for decrypting the pertinent portion of the packets. As stated above, Ho expressly states that the identifier database has the codes to decrypt the identifier portion of the data packet prepared and transmitted by the source terminal. Ho also expressly states

that the data access request is encrypted using a code readable only by the data request database. Interestingly, by including these statements, Ho effectively teaches away from the need to include encryption key identification information within the packets because such identification is unnecessary when the receiving components already know the encryption codes. Thus, the data packets discussed in Ho do not suggest a database structure having at least one encryption key identification in association with a data entity and corresponding to the encryption key used to encrypt the data entity.

For at least the reasons asserted, claim 1 is not anticipated or rendered obvious by Ho. Instead, Applicant believes claim 1 is in allowable form and respectfully requests that it be allowed in a timely fashion. Claims 2-27 depend from claim 1. Because claim 1 is in allowable form, the claims that depend from claim 1 are also in allowable form for at least the reasons asserted. Thus, Applicant respectfully requests that claims 2-27 also be allowed in a timely fashion.

Claim 28

The action rejected independent claim 28 pursuant to 35 U.S.C. § 102 as being anticipated by Ho. Because Ho fails to set forth each and every element of this claim, Applicant respectfully traverses this rejection.

Claim 28 is directed to a computer readable data transmission medium containing a data structure for encrypted data. The data structure of claim 28 is similar to the database structure of claim 1 in that it comprises at least one data entity encrypted by at least one encryption key, the data entity having at least one searchable attribute, and at least one encryption key identification in association with the data entity and corresponding to the encryption key.

As stated above, Ho describes data packets that are prepared and transmitted and describes the information contained in the data packets. While these data packets do contain encrypted data, they do not contain any encryption key identification information in association with the encrypted data and corresponding to the encryption key used to encrypt the data. Again, in the Ho system it is simply unnecessary to transmit any encryption key identification information because the receiving components already know the codes. If the data packets do not contain an encryption key identification, then there is no transmission medium containing such information. Therefore, Ho does not disclose, teach, or suggest the transmission medium of claim 28.

For at least the reasons stated, Ho does not anticipate claim 28. Instead, Applicant believes claim 28 is in allowable form and respectfully requests that it be allowed in a timely fashion.

Claim 29

The action rejected independent claim 29 pursuant to 35 U.S.C. § 103 as being unpatentable over Ho in view of Matyas. In order for these references to render the claim obvious, at a minimum there must be some suggestion or motivation to modify or combine the references, there must be some reasonable expectation of success, and the references must teach or suggest each and every limitation of the claim. As explained below, the combination of Ho in view of Matyas fails in these minimum requirements, and, therefore, Applicant respectfully traverses this rejection.

Claim 29 is directed to a computer readable data transmission medium containing a data structure for encrypted data. The data structure comprises a plurality of data entities encrypted by at least one encryption key having an encryption key identification and at least one system key common name corresponding to a system key operable to encrypt the encryption key identification. Thus, the data structure of claim 29 contains both encrypted data entities and information associated

with the data entities that will lead to the identity of the encryption key used to encrypt the data entities.

Matyas is directed to a cryptographic method for discouraging the copying and sharing of purchased software programs. Generally, in the first step of the method a software vendor encrypts a program using a unique file key and then copies the encrypted program to a disk. The vendor also adds a serial number, a program number, and an authorization number, which is the program number and serial number encrypted using a secret key, to the disk. Thereafter, a purchaser desiring to use the program will contact the vendor for a password and provide the serial number, the program number, and the authorization number from the disk and the purchaser's computer or smart card number (the smart card may be provided with the program disk by the vendor). The vendor recreates the authorization number and verifies that the authorization number provided by the purchaser is valid. If it is, the vendor provides the serial number, program number, and computer/smart card number to a key distribution center and requests a password. The center produces a unique cryptography key that it sends back to the vendor. In one embodiment, the center encrypts the computer/smart card number using a universal key and then uses this encrypted number as the key to encrypt the serial number and program number to produce the cryptography key. (Col. 6, lines 44-52.) In another embodiment, the center may use the smart card number to look up a corresponding encryption key that it then uses to encrypt the serial number and program number to produce the cryptography key. (Col. 8, lines 45-49.) Thereafter, the vendor uses the cryptography key to encrypt the unique file key and thereby create the password that it provides to the purchaser. Upon receiving the password, the purchaser will create the cryptography key, use it to decrypt the password and obtain the unique file key, and then use the unique file key to decrypt the program file.

Neither Ho nor Matyas disclose, teach, or suggest a computer readable data transmission medium containing a data structure for encrypted data that comprises at least one system key common name corresponding to a system key operable to encrypt an encryption key identification. As stated above, Ho does disclose transmitting data packets containing encrypted data. Ho does not, however, disclose, teach, or suggest that the data packets also contain information that may be used to identify the key used to encrypt the data since it is simply unnecessary to transmit this type of information in the system described in Ho because the receiving components already know the codes.

Matyas describes the transmission of data (the serial numbers, program numbers and computer/smart card numbers) and encrypted data (the authorization numbers), the transmission of an encryption key (the cryptographic key), and the transmission of an encrypted encryption key (the password). None of the items transmitted in Matyas is a system key common name. This should be obvious with regard to the data and encrypted data. The authorization number is encrypted by a secret key known only to the vendor; the serial numbers, program numbers and computer/smart card numbers have nothing to do with the vendor's secret key and certainly are not the common name of the vendor's secret key. The cryptographic key is an actual encryption key and not the common name of an encryption key. The password is also an encryption key (although it must be decrypted before it can by used) and not the common name of an encryption key. To illustrate this point, consider that neither the cryptographic key nor the password require any other module, component, system, etc. in their use. In contrast, the system key common name is used to retrieve a system key from, for example, a table, so that the system key may be used to decrypt an encrypted encryption key identification which then may be used to retrieve an encryption key from, for example, another table, in order to decrypt the associated encrypted data. Because neither Ho nor Matyas disclose,

teach, or suggest a computer readable data transmission medium containing a data structure for encrypted data that comprises at least one system key common name, the combination of these references fails to teach or suggest each and every limitation of claim 29, and, therefore, fails to render claim 29 obvious.

Additionally, there is no motivation or suggestion in either Ho or Matyas to modify or combine these references. The system and method described in Ho are directed to protecting sensitive data by allowing only authorized users to view/manipulate the data. The system and method of Ho accomplish this by separating the identifier information from the data request information and encrypting these two sets of information using separate encryption keys with each key known only by a separate, isolated component. No encryption key is provided to the user to decrypt data. Instead, if the user is authorized, the data itself is sent to the user. In contrast, the system and method described in Matyas are directed to protecting and preventing unauthorized use of encrypted data in a purchaser's possession. The system and method of Matyas accomplish this by requiring the purchaser to request a password to unlock the encrypted data and by using separate, isolated components to generate the password. Once generated, the password is sent to the purchaser who then uses the password to decrypt the data. Clearly, the systems and methods of Ho and Matyas are incompatible: in Ho, the user requests to view/manipulate protected data not in his or her possession and the data is provided once it is determined that the user is authorized; in Matyas, the purchaser requests and receives a password to decrypt encrypted data in his or her possession. Thus, no person of ordinary skill in the art would look to Matyas to modify Ho.

The action asserts that the motivation for modifying the teachings of Ho with the teachings of Matyas is "to allow the user to decrypt and execute the program on any computer having a properly implemented and initialized encryption feature." Basically, the action is asserting that the

combination of Ho and Matyas either (1) would allow a user to receive encrypted data utilizing the system and method of Ho and then obtain the encryption key to decrypt the data utilizing the system and method of Matyas or (2) would allow a purchaser to buy an encrypted program that included instructions to initiate the system and method described by Ho, use the system and method of Matyas to obtain the decryption key for the program, and then use the Ho system and method to view/manipulate data located elsewhere. Regarding these options, it should be understood that the combination does not teach providing information that might lead to or identify the encryption key but, instead, teaches providing the actual key. Also, the combination does not teach encrypting the stored data and storing information that might lead to or identify the encryption key in association with the data. Clearly, neither of these possibilities teaches or suggests Applicant's invention.

Thus, for at least these reasons, claim 29 is rendered obvious by the combination of Ho and Matyas and is not unpatentable over Ho in view of Matyas. Instead, claim 29 is in allowable form, and Applicant respectfully requests that it be allowed in a timely fashion.

Claims 30-39

The action rejected independent claim 30 pursuant to 35 U.S.C. § 103 as being unpatentable over Ho in view of Matyas. Applicant respectfully traverses this rejection

Claim 30 is directed to a computer readable medium containing a database structure for storage of encrypted data. Two limitations apply to the database structure. First, the database structure comprises a plurality of data entities encrypted by at least one encryption key having an encryption key identification. Second, the database structure comprises at least one system key common name corresponding to a system key operable to encrypt the encryption key identification.

The combination of Ho and Matyas does not render claim 30 obvious for at least two reasons. First, the combination of Ho and Matyas does not teach or suggest each and every limitation of claim 30. Specifically, as described above, neither Ho nor Matyas disclose, teach, or suggest a computer readable data transmission medium containing a data structure for encrypted data that comprises at least one system key common name corresponding to a system key operable to encrypt an encryption key identification. Second, there is no motivation or suggestion in either Ho or Matyas to modify or combine these references as described above. Thus, for at least the reasons asserted, claim 30 is not unpatentable over Ho in view of Matyas. Instead, claim 30 is in allowable form, and Applicant respectfully requests that it be allowed in a timely fashion.

Claims 31-39 depend from claim 30. Because claim 30 is in allowable form, the claims that depend from claim 30 are also in allowable form for at least the reasons asserted. Thus, Applicant respectfully requests that claims 31-39 also be allowed in a timely fashion.

Claims 40-67

The action rejected independent claim 40 pursuant to 35 U.S.C. § 102 as being anticipated by Ho. Because Ho fails to set forth each and every element of this claim, Applicant respectfully traverses this rejection.

Claim 40 is directed to a method for storage and retrieval of encrypted data comprising three steps. The first step includes encrypting a data entity with an encryption key having an encryption key identification. The next step includes storing the data entity. Finally, the third step includes storing the encryption key identification in association with the data entity.

Ho does not disclose, teach or suggest the method of claim 40. Although the system discussed in Ho does include several databases, Ho does not specifically describe how information is

stored in those databases. Ho states only that the databases used in its system typically are tables that contain, for example, individually identifiable attributes, user access levels, and internal identifications, and describes using the contents of data packets to look up information in the tables. Ho does not include any additional information about the database contents and certainly does not discuss a step that includes encrypting the database contents. As discussed above, Ho actually teaches away from encrypting the information stored in the databases when it states that results from database queries may be encrypted before being transmitted to other sections of the system. If the information stored in the databases is already encrypted then there would be no need to encrypt that information again before it is transmitted.

Ho does describe preparing and transmitting data packets. While the steps described include encrypting the contents of the data packets, they do not include storing any encryption key identification information in association with the encrypted data and corresponding to the encryption key used to encrypt the data. Again, in the Ho system it is simply unnecessary to include any encryption key identification information in the data packets because the receiving components already know the codes. Therefore, Ho does not disclose, teach, or suggest the method of claim 40.

For at least the reasons asserted, claim 40 is not anticipated by Ho. Instead, claim 40 is in allowable form, and Applicant respectfully requests that it be allowed in a timely fashion. Claims 41-67 depend from claim 40. Because claim 40 is in allowable form, the claims that depend from claim 40 are also in allowable form for at least the reasons asserted. Thus, Applicant respectfully requests that claims 41-67 also be allowed in a timely fashion.

Claims 68-69

The action rejected independent claim 68 pursuant to 35 U.S.C. § 103 as being unpatentable over Ho in view of Matyas in further view of Kaufman and Alegre. The action fails to specifically state its reasoning for rejecting claim 68. Nonetheless, as explained below, the combination of these references fails to render claim 68 obvious, and, therefore, Applicant respectfully traverses this rejection.

Claim 68 is directed to a method for retrieval of encrypted data at rest. The method comprises: requesting a data manipulation using a searchable attribute; searching a plurality of data entities for matches to the searchable attribute; obtaining an encryption key identification from the data entities; searching for an encryption key using the encryption key identification; and decrypting the data entities with the encryption key.

Kaufman relates to cryptographic methods and systems which provide for secure communications against attackers. Generally, Kaufman discloses a system and method that includes encrypting a message using a large secret key. The secret key is then encrypted using the public key of the intended recipient. The secret key is also split into at least two partial keys, and a partial key that is just large enough to reduce the work factor sufficiently to make the key economically breakable is encrypted using the public key of an "authority." Thereafter, the encrypted message is sent along with the encrypted secret key and the encrypted partial key. When the recipient receives the message, it decrypts the secret key and uses that key to decrypt the message. An authority monitoring the transmission may decrypt the partial key and then use that partial key to assist in generating the full secret key so that it may decrypt the message.

Alegre relates to an apparatus and methods for authenticating a user for allowing access to resources on a trusted network. The apparatus and methods generally include creating a session key

the first time a user requests access to a resource on the network and storing the session key at the client's browser and at a key server. Subsequently, whenever the user accesses the trusted network during the session in which the session is made, the session key is transmitted with the access request so that the network can use the session key to authenticate the user. It should be understood that the session key disclosed in Alegre is not an encryption key. It merely is an unique number large enough so that it is infeasible to guess its value. (Col. 6, lines 56-58.)

The cited references do not disclose, teach or suggest a method that includes obtaining an encryption key identification from a data entity; searching for an encryption key using the encryption key identification; and decrypting the data entity with the encryption key. As discussed above, neither Ho nor Matyas disclose, teach or suggest storing an encryption key identification in association with a data entity. If no encryption key identification is stored in association with a data entity, then no encryption key identification can be obtained and used to search for an encryption key that may be used to decrypt the data entity.

Neither Kaufman nor Alegre provide the missing steps. Kaufman does not disclose storing encryption key identification for much the same reason as Ho, that is, the message, secret key, and partial secret key are encrypted using keys already known to the respective receiving parties. Again, if no encryption key identification is stored in association with a data entity, then no encryption key identification can be obtained and used to search for an encryption key that may be used to decrypt the data entity. The system and method of Alegre do not even discuss using encryption keys in the manner of Applicant's invention.

Additionally, there is no motivation or suggestion to combine the teachings of Kaufman or Alegre with the teachings of Ho and Matyas. Kaufman describes encrypting a message with an encryption key and providing means for an authority to obtain the encryption key in order to monitor

the message. Neither Ho nor Matyas discuss taking steps to allow an authority or any other entity to monitor their transmissions. There is no reason for the systems and methods of Ho and Matyas to include part of the key used to encrypt the message in the transmission of the message. Alegre utilizes a unique, unpredictable number to authenticate a user. It does not teach disclose using an encryption scheme to help authenticate the user. Thus, no person of ordinary skill in the art would look to Kaufman or Alegre to modify Ho or Matyas.

For at least the reasons asserted, claim 68 is not unpatentable over Ho in view of Matyas in further view of Kaufman and Alegre. Instead, claim 68 is in allowable form, and Applicant respectfully requests that it be allowed in a timely fashion. Claim 69 depends from claim 68. Because claim 68 is in allowable form, any claim that depends from claim 68 is also in allowable form for at least the reasons asserted. Thus, Applicant respectfully requests that claim 69 also be allowed in a timely fashion.

Claims 70-79

The action rejected independent claim 70 pursuant to 35 U.S.C. § 103 as being unpatentable over Ho in view of Matyas in further view of Kaufman and Alegre. The combination of these references fails to render claim 70 obvious as explained below, and, therefore, Applicant respectfully traverses this rejection.

Claim 70 is directed to a method for storage and retrieval of encrypted data. The method begins with encrypting a plurality of data entities with a rotating and dynamic encryption key having an encryption key identification. Next, the method includes storing the data entities. Third, the method includes creating and rotating to a new encryption key upon occurrence of a desired rotation event.

The cited references do not teach encrypting a plurality of data entities with a rotating and dynamic encryption key having an encryption key identification. As stated, in the systems and methods of Ho, Matyas, and Kaufman, the components or entities receiving transmissions already know the encryption keys. Thus, the references do not disclose, teach or suggest that their encryption keys have encryption key identification which may be utilized to identify the encryption keys. Although it does discuss using a session key, the session key of Alegre is not related to encryption keys. Additionally, as discussed above, there is no motivation or suggestion to combine the teachings of Kaufman or Alegre with the teachings of Ho and Matyas.

For at least the reasons asserted, claim 70 is not unpatentable over Ho in view of Matyas in further view of Kaufman and Alegre. Instead, claim 70 is in allowable form, and Applicant respectfully requests that it be allowed in a timely fashion. Claims 71-79 depend from claim 70. Because claim 70 is in allowable form, the claims that depends from claim 70 are also in allowable form for at least the reasons asserted. Thus, Applicant respectfully requests that claims 71-79 also be allowed in a timely fashion.

Claims 80-95

The action rejected independent claim 80 pursuant to 35 U.S.C. § 102 as being anticipated by Ho. Because Ho fails to set forth each and every element of this claim, Applicant respectfully traverses this rejection.

Claim 80 is directed to a computer system comprising an encryption key manager and an information database. The encryption key manager is operable to generate an encryption key having an encryption key identification, the encryption key being operable to encrypt a data entity. The

information database is operable to store the data entity in an encrypted form and to store the encryption key identification in association with the data entity.

Ho does not disclose, teach or suggest the system of claim 80. First, Ho does not disclose, teach or suggest an information database that is operable to store a data entity in an encrypted form. Although the system discussed in Ho does include several databases, Ho does not specifically describe how information is stored in those databases. Ho states only that the databases used in its system typically are tables that contain, for example, individually identifiable attributes, user access levels, and internal identifications, and describes using the contents of data packets to look up information in the tables. Ho does not include any additional information about the database contents and certainly does not discuss encrypting the database contents prior to storing that information. As discussed above, Ho actually teaches away from encrypting the information stored in the databases when it states that results from database queries may be encrypted before being transmitted to other sections of the system. If the information stored in the databases is already encrypted then there would be no need to encrypt that information again before it is transmitted.

Ho also does not disclose, teach or suggest an information database operable to store an encryption key identification in association with a data entity. As stated, Ho does not disclose, teach or suggest encrypting the entries of either the identifier or the data access request databases. If the entries are not encrypted, then there is no encryption key identification to store in association with the data entity.

Ho does describe preparing and transmitting data packets and states that the information in the data packets is encrypted. However, Ho does not disclose, teach, or suggest that the data packets include, or otherwise have associated with them, information regarding the identification of any encryption key. There is a simple reason for this: in the system described in Ho the components

receiving packets already know the codes for decrypting the pertinent portion of the packets. As stated above, Ho expressly states that the identifier database has the codes to decrypt the identifier portion of the data packet prepared and transmitted by the source terminal. Ho also expressly states that the data access request is encrypted using a code readable only by the data request database. Interestingly, by including these statements, Ho effectively teaches away from the need to include encryption key identification information within the packets because such identification is unnecessary when the receiving components already know the encryption codes. Thus, the data packets discussed in Ho do not suggest a database operable to store a data entity in an encrypted form and to store the encryption key identification in association with the data entity.

For at least the reasons asserted, claim 80 is not anticipated by Ho. Instead, claim 80 is in allowable form, and Applicant respectfully requests that it be allowed in a timely fashion. Claims 81-95 depend from claim 80. Because claim 80 is in allowable form, the claims that depend from claim 80 are also in allowable form for at least the reasons asserted. Thus, Applicant respectfully requests that claims 81-95 also be allowed in a timely fashion.

Claims 96-99

The action rejected independent claim 96 pursuant to 35 U.S.C. § 102 as being anticipated by Ho. Because Ho fails to set forth each and every element of this claim, Applicant respectfully traverses this rejection.

Claim 96 is directed to a computer readable medium containing instructions for controlling a computer system to encrypt and decrypt data. The instructions, which are similar to the steps of the method claimed in claim 40, include encrypting a data entity with an encryption key having an

encryption key identification, storing the data entity, and storing the encryption key identification in association with the data entity.

Ho does not disclose, teach or suggest the computer readable medium of claim 96. Although the system discussed in Ho does include several databases, Ho does not specifically provide instructions detailing how information is stored in those databases. Ho states only that the its databases may be tables that contain, for example, individually identifiable attributes, user access levels, and internal identifications, and describes using the contents of data packets to look up information in the tables. Ho does not include any additional information about the database contents and certainly does not discuss encrypting the database contents prior to storing that information. As discussed above, Ho actually teaches away from encrypting the information stored in the databases when it states that results from database queries may be encrypted before being transmitted to other sections of the system. If the information stored in the databases is already encrypted then there would be no need to encrypt that information again before it is transmitted.

Ho does describe preparing and transmitting data packets. While the steps described include encrypting the contents of the data packets, they do not include storing any encryption key identification information in association with the encrypted data and corresponding to the encryption key used to encrypt the data. Again, in the Ho system it is simply unnecessary to include any encryption key identification information in the data packets because the receiving components already know the codes.

Ho does not disclose, teach, or suggest the computer readable medium of claim 96. In particular, Ho does not disclose, teach, or suggest a computer readable medium that contains instructions for storing an encryption key identification in association with an encrypted data entity. Thus, for at least this reason, claim 96 is not anticipated by Ho. Instead, claim 96 is in allowable

form, and Applicant respectfully requests that it be allowed in a timely fashion. Claims 97-99 depend from claim 96. Because claim 96 is in allowable form, the claims that depend from claim 96 are also in allowable form for at least the reasons asserted. Thus, Applicant respectfully requests that claims 97-99 also be allowed in a timely fashion.

Claims 100-104

The action rejected independent claim 100 pursuant to 35 U.S.C. § 103 as being unpatentable over Ho in view of Matyas in further view of Kaufman and Alegre. As explained below, the combination of these references fails to render claim 100 obvious, and, therefore, Applicant respectfully traverses this rejection.

Claim 100 is directed to a method in a computer system for displaying customer information. First, the method includes receiving a request to view information from a user. Next, the method includes retrieving the information. The method then includes checking a security status of the information. Next, the method includes reviewing a security access list to find an identification corresponding to the user. Thereafter, the method includes checking a security access level of the user. Next, the method includes adapting display parameters to modify available display fields based on the security access level of the user. The method then includes displaying the permitted information and display fields based on the security access level of the user.

The cited references do not teach the method claimed in claim 100. In particular, the system and method of Ho do not disclose, teach, or suggest adapting display parameters to modify available display fields based on the security access level of the user and displaying the permitted information and display fields based on the security access level of the user. The system and method of Ho disclose sending the user the information if the user is permitted access. There is no further

discussion regarding paring the information down based on the user's access level or displaying only portions of the information based on the user's access level.

The remaining references do not provide the steps missing from the system and method disclosed in Ho so that the combination includes all of the steps claimed in claim 100. Matyas does not disclose checking to determine if the user entitled to view information and providing a partial portion of that information if appropriate. Matyas simply determines whether the user is authorized to receive the encryption key and sends the key if the user is so authorized. Kaufman also does not disclose such steps. Kaufman encrypts the message with secret key with the recipient's public key and sends the message. If the recipient is the actual authorized recipient, then it will have the appropriate key and be able to decrypt the message. Alegre assigns a session key if the user is authorized and, thereafter, so long as that session key is included the user may utilize the requested resources.

Thus, the combination of the cited references do not teach all of the limitations of claim 100. Additionally, as discussed above, there is no motivation or suggestion to combine the teachings of Kaufman or Alegre with the teachings of Ho and Matyas. Therefore, the cited references do not render claim 100 obvious.

For at least the reasons asserted, claim 100 is not unpatentable over Ho in view of Matyas in further view of Kaufman and Alegre. Instead, claim 100 is in allowable form, and Applicant respectfully requests that it be allowed in a timely fashion. Claims 101-104 depend from claim 100. Because claim 100 is in allowable form, the claims that depend from claim 100 are also in allowable form for at least the reasons asserted. Thus, Applicant respectfully requests that claims 101-104 also be allowed in a timely fashion.

Claims 105-110

The action rejected independent claim 105 pursuant to 35 U.S.C. § 103 as being unpatentable over Ho in view of Matyas in further view of Kaufman and Alegre. The action fails to specifically state its reasoning for rejecting claim 105. Nonetheless, the combination of these references fails to render claim 105 obvious as explained below, and, therefore, Applicant respectfully traverses this rejection.

Claim 105 is directed to a method in a computer system for communicating with an encryption server comprising: establishing communication with a general security manager of the encryption server; entering a request for manipulation of data; receiving a data entity in response to the request; retrieving security key information from the data entity; requesting an encryption key; receiving the encryption key; and decrypting the data entity.

The cited references do not teach retrieving security key information from a requested data entity, requesting an encryption key, receiving the encryption key, and decrypting the data entity. As stated, in the systems and methods of Ho, Matyas, and Kaufman, the components or entities receiving transmissions already know the encryption keys. Thus, the references do not disclose, teach or suggest that the encryption keys have security key information or that the components or entities must request such information or any encryption key. Although it does discuss using a session key, the session key of Alegre is not related to encryption keys and is not security key information. Moreover, Alegre does not involve requesting or receiving encryption keys or decrypting data. Additionally, as discussed above, there is no motivation or suggestion to combine the teachings of Kaufman or Alegre with the teachings of Ho and Matyas.

For at least the reasons asserted, claim 105 is not unpatentable over Ho in view of Matyas in further view of Kaufman and Alegre. Instead, claim 105 is in allowable form, and Applicant

respectfully requests that it be allowed in a timely fashion. Claims 106-110 depend from claim 105. Because claim 105 is in allowable form, the claims that depend from claim 105 are also in allowable form for at least the reasons asserted. Thus, Applicant respectfully requests that claims 106-110 also be allowed in a timely fashion.

Claims 111-120

The action rejected independent claim 111 pursuant to 35 U.S.C. § 103 as being unpatentable over Ho in view of Matyas.

Claim 111 is directed to an encryption and decryption method for encrypting and decrypting data. The method comprises two steps. First, the method comprises encrypting data with an encryption key having an encryption key identification. Next, the method comprises encrypting the encryption key identification with a system key having a system key common name.

The combination of Ho and Matyas does not render claim 111 obvious for at least two reasons. First, the combination of Ho and Matyas does not teach or suggest each and every limitation of claim 111. Specifically, neither Ho nor Matyas disclose, teach, or suggest encrypting the encryption key identification with a system key having a system key common name because neither Ho nor Matyas disclose, teach or suggest in any way that an encryption key may be referred to by a common name. There is no reason in the Ho system and method to provide any sort of reference for encryption keys, such as a common name, since all of the components know the pertinent keys. In the Matyas system and method, encryption keys are created, utilized and/or transmitted. There is no discussion, however, of assigning or associating a reference name to a particular key and then using that name to refer to or look up the key. The keys associated with a smart card may be looked up, but the card number is used for this operation and not a common

name. Second, and no less important, there is no motivation or suggestion in either Ho or Matyas to modify or combine these references as described above.

Thus, for at least the reasons asserted, claim 111 is not unpatentable over Ho in view of Matyas. Instead, claim 111 is in allowable form, and Applicant respectfully requests that it be allowed in a timely fashion. Claims 112-120 depend from claim 111. Because claim 111 is in allowable form, the claims that depend from claim 111 are also in allowable form for at least the reasons asserted. Thus, Applicant respectfully requests that claims 112-120 also be allowed in a timely fashion.

Conclusion

For at least the reasons asserted above, the cited references do not anticipate or render unpatentable claims 1-120 as amended. Applicant believes that each and every claim asserted in his application is in patentable form and, therefore, respectfully requests that those claims be allowed in a timely fashion.

The above Amendment is fully responsive to the office action dated September 1, 2004. If there are any matters which can be further clarified by telephone, the Examiner is requested to contact the undersigned attorney.

The Office is authorized to charge any fees due or credit any overpayments in connection with the filing of this paper to Deposit Account No. 50-0354.

Dated: 2/28/2005

Christopher J. Eaton

Christopher J. Eaton, Reg. No. 51,143
Spencer Fane Britt & Browne LLP
1000 Walnut, Suite 1400
Kansas City, MO 64106
Tele.: 816-474-8100